View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Advances in Mathematics 217 (2008) 282–304

ADVANCES IN Mathematics

www.elsevier.com/locate/aim

Commutative presemifields and semifields

Robert S. Coulter [a,*], Marie Henderson [b]

[a] *Department of Mathematical Sciences, Ewing Hall, University of Delaware, Newark, DE 19716, USA*
[b] *310/60 Willis street, Te Aro (Wellington) 6001, New Zealand*

Received 1 April 2006; accepted 5 July 2007

Available online 18 September 2007

Communicated by Michael J. Hopkins

Abstract

Strong conditions are derived for when two commutative presemifields are isotopic. It is then shown that any commutative presemifield of odd order can be described by a planar Dembowski–Ostrom polynomial and conversely, any planar Dembowski–Ostrom polynomial describes a commutative presemifield of odd order. These results allow a classification of all planar functions which describe presemifields isotopic to a finite field and of all planar functions which describe presemifields isotopic to Albert's commutative twisted fields. A classification of all planar Dembowski–Ostrom polynomials over any finite field of order p^3, p an odd prime, is therefore obtained. The general theory developed in the article is then used to show the class of planar polynomials $X^{10} + aX^6 - a^2X^2$ with $a \neq 0$ describes precisely two new commutative presemifields of order 3^e for each odd $e \geqslant 5$.
© 2007 Elsevier Inc. All rights reserved.

MSC: primary 12K10, 17A35; secondary 51A35, 51A40

Keywords: Commutative semifield; Dembowski–Ostrom polynomial; Planar function

1. Introduction

A *semifield* is a ring with no zero-divisors, a multiplicative identity and left and right distributivity. A semifield need not be commutative nor associative. In the finite case, however, it follows from Wedderburn's Theorem, [23], that associativity implies commutativity. A non-associative finite commutative semifield is therefore the nearest algebraic structure to a finite field (which

* Corresponding author.
E-mail address: coulter@math.udel.edu (R.S. Coulter).

0001-8708/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.aim.2007.07.007

is not a finite field). While the classification of finite fields has been complete for many years (uniqueness was established in 1893 by Moore, [19,20]), no classification of finite commutative semifields exists nor does it appear that such a classification is currently within reach.

A *presemifield* is a semifield which does not necessarily have a multiplicative identity (throughout, the term presemifield will not preclude the possibility of an identity, unless specifically stated). There is a well-known correspondence, via coordinatisation, between presemifields and translation planes of Lenz–Barlotti type V.1 and above. Planar functions were introduced by Dembowski and Ostrom in [8] to describe affine planes possessing a collineation group with specific properties. In particular, they noted that every commutative semifield of odd order can be described by a planar function, see [8, p. 257]. This comment is essentially the motivation for this article. Our aim is to show that a unified treatment of commutative presemifields of odd order can be achieved through the medium of planar Dembowski–Ostrom polynomials. As part of the development, we give stronger conditions than those previously known for isotopism of commutative presemifields of any order (this is equivalent to the question of isomorphism of the corresponding projective planes).

Let $\mathbb{F}_q$ denote the finite field of $q = p^e$ elements, p an odd prime, $\mathbb{F}_q^*$ denote the non-zero elements of $\mathbb{F}_q$, and $\mathbb{F}_q[X]$ denote the ring of polynomials in indeterminate X over $\mathbb{F}_q$. Recall that any function mapping $\mathbb{F}_q$ to $\mathbb{F}_q$ can be represented by a polynomial of degree less than q (this is immediate from the Lagrange interpolation formula). A *permutation* polynomial over $\mathbb{F}_q$ is a polynomial which, under evaluation, induces a bijective mapping on $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[X]$ is called *planar* if and only if for every $a \in \mathbb{F}_q^*$, the difference polynomial $\Delta_f(X, a) = f(X + a) - f(X) - f(a)$ is a permutation polynomial over $\mathbb{F}_q$. More generally, for groups G and H, written additively, but not necessarily abelian, a function $\phi : G \to H$ is called a *planar function* if for each non-identity $a \in G$, the mapping $\lambda_a(x) = \phi(a + x) - \phi(x)$ is a bijection.

Two classes of polynomials play a central role in all that follows. Any linear transformation of $\mathbb{F}_q$ can be represented by a polynomial $L \in \mathbb{F}_q[X]$ with the shape

$$L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}.$$

Such polynomials are called *linearised polynomials* (they are also called additive polynomials or p-polynomials). For any $x, y \in \mathbb{F}_q$, $L(x + y) = L(x) + L(y)$ and any polynomial of degree less than q satisfying this additive property is necessarily a linearised polynomial. Note also that $L(\alpha x) = \alpha L(x)$ for all $\alpha \in \mathbb{F}_p$ and $x \in \mathbb{F}_q$. Further, L is a permutation polynomial over $\mathbb{F}_q$ (a non-singular linear transformation of $\mathbb{F}_q$) if and only if $x = 0$ is the only root of L in $\mathbb{F}_q$. Linearised polynomials are closed with respect to composition and reduction modulo $X^q - X$. The compositional inverse, modulo $X^q - X$, of a linearised permutation polynomial L over $\mathbb{F}_q$ shall be denoted by $L^{-1}(X)$. A *Dembowski–Ostrom* (*DO*) *polynomial* $D \in \mathbb{F}_q[X]$ is a polynomial with the shape

$$D(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}.$$

In odd characteristic, DO polynomials are closed under composition with linearised polynomials and under reduction modulo $X^q - X$.

The additive group of a finite presemifield is necessarily an elementary abelian p-group, see [16, Section 2.4] for a simple proof. Consequently, any finite presemifield can be represented

by $\mathcal{R} = (\mathbb{F}_q, +, \star)$. Here $(\mathbb{F}_q, +)$ is the additive group of $\mathbb{F}_q$ and $x \star y = \psi(x, y)$ where ψ is a function mapping $\mathbb{F}_q \times \mathbb{F}_q$ onto $\mathbb{F}_q$.

As mentioned, there is a correspondence between commutative presemifields and translation planes of Lenz–Barlotti type V.1 and above. It was shown by Albert, [2], that two presemifields coordinatise isomorphic planes if and only if they are *isotopic*. To be precise, let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be two presemifields. Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three linearised permutation polynomials $L, M, N \in \mathbb{F}_q[X]$ such that

$$\forall x, y \in \mathbb{F}_q\colon\ M(x) \star N(y) = L(x * y).$$

We say that the triple (M, N, L) is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$. In Section 2 we consider isotopism for commutative presemifields. For isotopic commutative presemifields, it appears natural to expect the existence of an isotopism of the form (N, N, L). We show this is indeed the situation in most cases. Even in the cases where this fails, restrictive conditions on the possible isotopisms can be obtained. For our strongest result in this direction see Theorem 2.6.

We then restrict ourselves to finite commutative semifields of odd order. The observation of Dembowski and Ostrom, noted above, implies any finite commutative semifield of odd order can be described by a planar polynomial over a finite field. Our next result determines those planar polynomials which describe commutative presemifields of odd order, see Theorem 3.3. This allows us to show that the problem of classifying commutative presemifields of odd order is equivalent to classifying all planar DO polynomials. Combined with our results on isotopism, this yields several important corollaries. We obtain a description of all planar polynomials which describe a presemifield isotopic to a finite field. This was previously known only for presemifields of order p or p^2. Further, by applying a result of Menichetti, [18], a classification of planar DO polynomials over $\mathbb{F}_{p^3}$ is also obtained. We end the section by defining an equivalence relation on planar DO polynomials (effectively with linearised permutation polynomials under reduction modulo $X^q - X$). This relation appears to be particularly relevant to the isotopism problem for commutative presemifields, as any equivalence class of this relation consists entirely of planar DO polynomials describing isotopic presemifields of a given order.

Only a small number of commutative semifields of odd order have been found (until the recent article of Kantor, [15], the same was true for commutative semifields of even order). The confirmed distinct classes are as follows:

(i) The Dickson semifields, [9].
(ii) The commutative twisted fields of Albert, [1].
(iii) The Cohen–Ganley semifields, [5].
(iv) The Ganley semifields, [11].
(v) The Penttila–Williams semifield of order 3^{10}, [21].

A potential sixth class exists corresponding to a class of planar DO polynomials introduced by Coulter and Matthews in [7] and extended by Ding and Yuan, [10]. The theory developed in this article allows us to show that this potential is realised. The polynomial $X^{10} + X^6 - X^2 \in \mathbb{F}_{3^e}[X]$ was shown to be planar if and only if e is odd or $e = 2$ in [7]. The corresponding commutative semifields have been called, in various places, the Coulter–Matthews semifields, though until now they were not known to be distinct, isotopically, from finite fields or Albert's twisted fields. This class of planar polynomials was extended in [10], where it is shown $X^{10} + aX^6 - a^2X^2 \in \mathbb{F}_{3^e}[X]$ with $a \neq 0$ is planar if e is odd or $e = 2$ and $a = \pm 1$. In Section 4 we first show these conditions

are sufficient and note any two squares of $\mathbb{F}_{3^e}^*$ generate isotopic commutative presemifields, as do any two non-squares, see Theorem 4.2. We then show the two cases $a = 1$ and $a = -1$, corresponding to the square and non-square cases, yield commutative semifields isotopically distinct from all known commutative semifields and each other. Thus, the final result of this article establishes the existence of two new affine translation planes (Lenz–Barlotti type V.1) of order 3^e for all odd $e \geqslant 5$.

2. Isotopy of commutative presemifields of any order

We call an isotopism of the form (N, N, L) a *strong isotopism* (or weak isomorphism) and say two commutative presemifields are *strongly isotopic* if there exists a strong isotopism between them. We begin with the trivial but useful

Lemma 2.1. *Let $\mathcal{R} = (\mathbb{F}_q, +, *)$ be a commutative presemifield and suppose $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ is any presemifield isotopic to $\mathcal{R}$. Any isotopism (M, N, L) from $\mathcal{R}_1$ to $\mathcal{R}$ must satisfy*

$$M(x) \star N(y) = M(y) \star N(x)$$

for all $x, y \in \mathbb{F}_q$.

Proof. This is immediate from the commutativity of $\mathcal{R}$.

Theorem 2.2. *Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields. Then there exists an isotopism (M, N, L) between $\mathcal{R}_1$ and $\mathcal{R}_2$ such that either*

(i) *$M = N$, or*
(ii) *$M(x) \neq N(\alpha x)$ for all $\alpha \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_q^*$.*

Proof. Let (M, N, L) be an isotopism from $\mathcal{R}_1$ to $\mathcal{R}_2$. Suppose $M \neq N$ and that there exists $x_0 \in \mathbb{F}_q^*$ and $\alpha \in \mathbb{F}_p^*$ such that $M(x_0) = N(\alpha x_0)$. As $\alpha \in \mathbb{F}_p^*$, we have

$$(\alpha x) \star y = \alpha(x \star y) = x \star (\alpha y)$$

for all $x, y \in \mathbb{F}_q$. Using Lemma 2.1, it follows that

$$M(x) \star N(\alpha y) = M(y) \star N(\alpha x)$$

holds for all $x, y \in \mathbb{F}_q$. Set $y = x_0$. For all $x \in \mathbb{F}_q$, we have

$$\begin{aligned} M(x) \star N(\alpha x_0) &= M(x) \star M(x_0) \\ &= M(x_0) \star N(\alpha x) \\ &= N(\alpha x) \star M(x_0). \end{aligned}$$

As $M(x_0) = N(\alpha x_0)$, cancelling yields $M(x) = N(\alpha x)$ for all $x \in \mathbb{F}_q$. Hence $M(X) = \alpha N(X)$. It follows that

$$N(x) \star N(y) = \alpha^{-1} L(x * y)$$

for all $x, y \in \mathbb{F}_q$. Thus $(N, N, \alpha^{-1}L)$ is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$, which satisfies case (i) of our statement. □

Consider the three subsets of a semifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$

$$\mathcal{N}_l(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathcal{R}\},$$
$$\mathcal{N}_m(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathcal{R}\},$$
$$\mathcal{N}_r(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathcal{R}\}.$$

These are known as the left, middle and right nucleus, respectively. It is easily shown that these sets are finite fields. The set $\mathcal{N}(\mathcal{R}) = \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r$ is called the nucleus. In a sense, the nuclei measure how far $\mathcal{R}$ is from being associative, and hence a field. Clearly, if $\mathcal{R}$ is commutative, then the left and right nuclei are the same. The orders of the respective nuclei are invariants under isotopism.

Let $\mathcal{R} = (\mathbb{F}_q, +, \star)$ be a commutative presemifield which does not contain an identity. To create a semifield from $\mathcal{R}$ choose any $a \in \mathbb{F}_q^*$ and define a new multiplication $*$ by

$$(x \star a) * (a \star y) = x \star y$$

for all $x, y \in \mathbb{F}_q$. Then $\mathcal{R}' = (\mathbb{F}_q, +, *)$ is a commutative semifield isotopic to $\mathcal{R}$ with identity $a \star a$. We say $\mathcal{R}'$ is a commutative semifield *corresponding to* the commutative presemifield $\mathcal{R}$. In particular, as $\mathcal{R}$ is commutative, the mapping $x \mapsto x \star a = a \star x = L_a(x)$ is a non-singular linear transformation dependent only on a and can be represented by a linearised permutation polynomial L_a. An isotopism between $\mathcal{R}$ and $\mathcal{R}'$ is the strong isotopism $(L_a(X), L_a(X), X)$. Consequently, we now derive results for commutative semifields, where the existence of subfields (sub-rings which are fields) allows much stronger results.

Theorem 2.3. *Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then every isotopism (M, N, L) between $\mathcal{R}_1$ and $\mathcal{R}_2$ satisfies either*

(i) *$M = N$, or*
(ii) *$M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$ where $\alpha \in \mathcal{N}_m(\mathcal{R}_1)$.*

Proof. Suppose $M \neq N$. Denote the identity of $\mathcal{R}_1$ by ϵ and suppose $N(b) = \epsilon$. Set $\alpha = M(b)$. By Lemma 2.1,

$$M(x) \star N(b) = M(x) = M(b) \star N(x) = \alpha \star N(x)$$

for all $x \in \mathbb{F}_q$. Therefore $M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$. It remains to show $\alpha \in \mathcal{N}_m(\mathcal{R}_1)$. Again by Lemma 2.1, for all $x, y \in \mathbb{F}_q$, we have $M(x) \star N(y) = M(y) \star N(x)$ and so

$$\begin{aligned}\big(\alpha \star N(x)\big) \star N(y) &= \big(N(x) \star \alpha\big) \star N(y) \\ &= \big(N(y) \star \alpha\big) \star N(x) \\ &= N(x) \star \big(\alpha \star N(y)\big)\end{aligned}$$

for all $x, y \in \mathbb{F}_q$. As N is a permutation polynomial, we have $\alpha \in \mathcal{N}_m(\mathcal{R}_1)$ as required. □

Theorem 2.4. *Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then there exists an isotopism (M, N, L) between $\mathcal{R}_1$ and $\mathcal{R}_2$ such that either*

(i) *$M = N$, or*
(ii) *$M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$ where $\alpha \in \mathcal{N}_m(\mathcal{R}_1) \setminus \mathcal{N}(\mathcal{R}_1)$.*

Proof. By Theorem 2.3, we need only consider the case $M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$ with $\alpha \in \mathcal{N}(\mathcal{R}_1)$. In this case, we have

$$\begin{aligned} M(x) \star N(y) &= \big(\alpha \star N(x)\big) \star N(y) \\ &= \alpha \star \big(N(x) \star N(y)\big). \end{aligned}$$

For any semifield $\mathcal{R} = (\mathbb{F}_q, +, \times)$, for fixed $a \in \mathbb{F}_q^*$, we have $a \times x = L_a(x)$ for some linearised permutation polynomial L_a dependent on a. In particular, here we have

$$L(x \star y) = M(x) \star N(y) = L_\alpha\big(N(x) \star N(y)\big)$$

for some linearised permutation polynomial L_α. By composing with L_α^{-1}, it follows that $(N, N, L_\alpha^{-1}(L))$ is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$, which is an example of case (i). □

Theorem 2.5. *Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then there exists an isotopism (M, N, L) between $\mathcal{R}_1$ and $\mathcal{R}_2$ such that either*

(i) *$M = N$, or*
(ii) *$M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$ where $\alpha \in \mathcal{N}_m(\mathcal{R}_1) \setminus \mathcal{N}(\mathcal{R}_1)$ cannot be written in the form $\alpha = \gamma \star \beta^2$ where $\gamma \in \mathcal{N}(\mathcal{R}_1)$ and $\beta \in \mathcal{N}_m(\mathcal{R}_1)$.*

Proof. Following on from Theorem 2.4, assume $M(X) \equiv \alpha \star N(X) \bmod (X^q - X)$ with $\alpha \in \mathcal{N}_m(\mathcal{R}_1) \setminus \mathcal{N}(\mathcal{R}_1)$. Suppose $\alpha = \gamma \star \beta^2$ where $\gamma \in \mathcal{N}(\mathcal{R}_1)$ and $\beta \in \mathcal{N}_m(\mathcal{R}_1)$. Then for all $x, y \in \mathbb{F}_q$, we have

$$\begin{aligned} L(x * y) &= \big(\big(\gamma \star \beta^2\big) \star N(x)\big) \star N(y) \\ &= \gamma \star \big(\big(\beta^2 \star N(x)\big) \star N(y)\big) \\ &= \gamma \star \big(\big(N(x) \star \beta^2\big) \star N(y)\big) \\ &= \gamma \star \big(N(x) \star \beta\big) \star \big(\beta \star N(y)\big) \\ &= \gamma \star \big(\beta \star N(x)\big) \star \big(\beta \star N(y)\big). \end{aligned}$$

Hence $L'(x * y) = N'(x) \star N'(y)$ for all $x, y \in \mathbb{F}_q$, where $L'(X) \equiv \gamma^{-1} \star L(X) \bmod (X^q - X)$ and $N'(X) \equiv \beta \star N(X) \bmod (X^q - X)$. So (N', N', L') is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$. Now if α is a square in $\mathcal{N}_m(\mathcal{R}_1)$, then $\alpha = \beta^2 = 1_{\mathcal{R}_1} \star \beta^2$ and we can generate a strong isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$ using the approach just given. □

With this last result in place, we may now prove the key theorem of this section.

Theorem 2.6. *Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields of characteristic p. Suppose the order of the middle nuclei and nuclei of corresponding commutative semifields is p^m and p^n, respectively. One of the following statements must hold.*

(i) *m/n is odd and $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.*
(ii) *m/n is even and either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between any two corresponding commutative semifields $\mathcal{R}_1'$ and $\mathcal{R}_2'$ are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1')$.*

Proof. Firstly, recall that we may convert any commutative presemifield to a commutative semifield via a strong isotopism. So if the commutative semifields are strongly isotopic, so too are the commutative presemifields. If $m/n = 1$, then it follows from Theorem 2.4 that any corresponding commutative semifields of $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic. If $m > n$, then in the corresponding semifields the nucleus is a proper subfield of the middle nucleus. Theorem 2.5 shows that the problem reduces to whether the nucleus contains both squares and non-squares of the middle nucleus. If m/n is odd, then the nucleus does contain both squares and non-squares of the middle nucleus and any element α in the middle nucleus can be written as $\gamma \star \beta^2$, proving (i). If m/n is even, then the nucleus will contain only squares of the middle nucleus, and any non-square cannot be written in the desired form. Theorems 2.3 and 2.5 together imply either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic, or the only isotopisms between their corresponding commutative semifields must be of the form $(\alpha \star N, N, L)$ where α is a non-square element of the middle nucleus of the semifield corresponding to $\mathcal{R}_1$. This proves (ii). □

The theorem yields several corollaries.

Corollary 2.7. *Any two commutative presemifields of even order are isotopic if and only if they are strongly isotopic.*

Proof. Every element in a finite field of even order is a square, so the second possibility of Theorem 2.6(ii) cannot occur. □

Corollary 2.8. *Any two commutative presemifields of order p^e with e odd are isotopic if and only if they are strongly isotopic.*

Proof. Under the hypothesis, only Theorem 2.6(i) applies. □

3. Commutative presemifields of odd order

Throughout the remainder of the article we assume q is odd. Let $f \in \mathbb{F}_q[X]$ be any polynomial. Define an incidence structure $I(f)$ as follows: points are the elements of $\mathbb{F}_q \times \mathbb{F}_q$, lines are the symbols $\mathcal{L}(a, b)$ with $a, b \in \mathbb{F}_q$, together with the symbols $\mathcal{L}(c)$ with $c \in \mathbb{F}_q$. Incidence is defined by

$$(x, y) \in \mathcal{L}(a, b) \quad \text{if and only if} \quad y = f(x - a) + b; \qquad \text{and}$$
$$(x, y) \in \mathcal{L}(c) \quad \text{if and only if} \quad x = c.$$

The next result is a specialisation of [8, Lemma 12].

Lemma 3.1. *The polynomial $f \in \mathbb{F}_q[X]$ is planar if and only if $I(f)$ is an affine plane.*

It was shown in [7] that for any planar polynomial $f \in \mathbb{F}_q[X]$ and any $c \in \mathbb{F}_q$, the planes $I(f(X))$ and $I(f(X) + c)$ are isomorphic. Hence, without loss of generality, we may assume $f(0) = 0$.

Let $f \in \mathbb{F}_q[X]$ be a planar polynomial with $f(0) = 0$. Define a second plane $\Pi(f)$ as follows. The points of the plane are the elements of $\mathbb{F}_q \times \mathbb{F}_q$, and the lines of one parallel class are described by the equations $x = c$ for each $c \in \mathbb{F}_q$. For $x_1, x_2 \in \mathbb{F}_q$, define $x_1 \star x_2 = f(x_1 + x_2) - f(x_1) - f(x_2) = \Delta_f(x_1, x_2)$. Then, for each $a, b \in \mathbb{F}_q$, the remaining lines of $\Pi(f)$ are given by the equations $y = x \star a + b$. Since $x \star 0 = 0$, it follows that $y = c$ is the equation of a line in $\Pi(f)$ for all $c \in \mathbb{F}_q$. It is easily verified that $\Pi(f)$ is an affine plane. The mapping $(x, y) \mapsto (x, y + f(x))$ maps lines of $I(f)$ to $\Pi(f)$. It is readily seen that this map is invertible and so $I(f)$ and $\Pi(f)$ are isomorphic. We summarise this with

Lemma 3.2. *Let $f \in \mathbb{F}_q[X]$ be a planar polynomial with $f(0) = 0$. Then $\Pi(f)$ and $I(f)$ are isomorphic.*

For a planar polynomial $f \in \mathbb{F}_q[X]$, define $\mathcal{R}_f = (\mathbb{F}_q, +, \Delta_f)$ to be the algebraic structure with field addition and multiplication defined by $x \star y = \Delta_f(x, y)$ for all $x, y \in \mathbb{F}_q$. We note that in the case where $I(f)$ and $\Pi(f)$ define translation planes, $\mathcal{R}_f$ will be a presemifield (existence of an identity is not guaranteed). This is immediate from [7, Corollary 5.10], which states that the translation line in such cases must be the line at infinity.

Our next result shows that any semifield plane described by a planar function can be described by a planar DO polynomial, and vice versa. Further, any such semifield is necessarily commutative.

Theorem 3.3. *If $\mathcal{P}$ is a semifield plane of order n described by a planar function, then $n = q = p^e$, for some odd prime p, the semifield is commutative, and there exists a planar Dembowski–Ostrom polynomial $D \in \mathbb{F}_q[X]$ such that $\mathcal{P}$ and $I(D)$ are isomorphic. Conversely, every planar Dembowski–Ostrom polynomial describes a commutative semifield plane.*

The proof relies fundamentally on the characterisation of DO polynomials given by Coulter and Matthews, [7, Theorem 3.2].

Lemma 3.4. *Let $f \in \mathbb{F}_q[X]$ with degree less than q. The following statements are equivalent.*

(i) *$f = D + L$, where D is a Dembowski–Ostrom polynomial and L is a linearised polynomial.*
(ii) *For each $a \in \mathbb{F}_q^*$, $\Delta_f(X, a)$ is a linearised polynomial.*

Note that the statement given here differs slightly from that given in [7]. This results from a change in the definition of the difference polynomial.

Proof of Theorem 3.3. Suppose D is a planar Dembowski–Ostrom polynomial. It is easily seen that the multiplication defined by $x \star y = \Delta_D(x, y)$ is commutative. From Lemma 3.4, $X \star y = y \star X = \Delta_D(X, y)$ is a linearised permutation polynomial for each $y \in \mathbb{F}_q^*$. From the properties of linearised polynomials, it follows that we have the full two-sided distributive law

and that there are no zero-divisors. Therefore $\mathcal{R}_D$ is a presemifield and so $I(D)$ is a semifield plane.

Now suppose a planar function describes a semifield plane $\mathcal{P}$. The additive group of the presemifield coordinatising $\mathcal{P}$ is necessarily elementary abelian and so we can construct a planar polynomial $f \in \mathbb{F}_q[X]$ which describes the same plane. Without loss of generality, let $f \in \mathbb{F}_q[X]$, with $f(0) = 0$, be a planar polynomial defining the semifield plane $\mathcal{P}$. It follows that $\mathcal{R}_f$ defines the (necessarily commutative) presemifield. Since the distributive laws hold, for each $a \in \mathbb{F}_q^*$, $X \star a = \Delta_f(X, a)$ is a linearised permutation polynomial. By Lemma 3.4, we must have $f = D + L$, where D is a planar DO polynomial, and L is a linearised polynomial. Note, however, that $\Delta_f(X, Y) = \Delta_D(X, Y)$. So we may describe the commutative semifield plane by the planar DO polynomial D instead. This establishes the result. □

We note that [14, Proposition 3.7] is a consequence of Theorems 3.3 and 2.3.

Theorem 3.3 completely classifies those planar polynomials which represent commutative presemifields. As both linearised polynomials and DO polynomials are closed under reduction modulo $X^q - X$, a planar polynomial $f \in \mathbb{F}_q[X]$ represents a commutative presemifield of order q if and only if $f(X) = D(X) + L(X) + c$ where D is a planar DO polynomial, L is any linearised polynomial, and $c \in \mathbb{F}_q$ is a constant.

As mentioned in the introduction, few distinct commutative semifields of odd order are known. It is therefore not surprising that the number of planar DO polynomials identified is also small. They can be summarised as follows:

(i) For any finite field of odd characteristic, the polynomial $f(X) = X^2 + aX + b$ is a planar polynomial for all a and b. In this case, the corresponding presemifield is isotopic to a finite field. In fact, if $f(X) = \frac{1}{2}X^2$, then $\mathcal{R}_f = \mathbb{F}_q$. It was shown independently in [12,13,22] that any planar polynomial over a prime field is necessarily a quadratic (under reduction modulo $X^p - X$). Additionally, any planar monomial X^n over $\mathbb{F}_{p^2}$ is necessarily either X^2 or X^{2p} (under reduction modulo $X^{p^2} - X$), see [6].

(ii) Let $f(X) = X^{p^\alpha + 1}$ be defined over $\mathbb{F}_{p^e}$ for odd prime p. Then f is a planar polynomial if and only if $e/(\alpha, e)$ is odd (where (α, e) denotes the greatest common divisor of α and e), see [7, Theorem 3.3]. In such cases, the resulting presemifield is isotopic to the commutative twisted fields generated by the field automorphism X^{p^α} defined by Albert in [1].

(iii) Let $a \in \mathbb{F}_{3^e}^*$. Then $X^{10} + aX^6 - a^2X^2$ is planar over $\mathbb{F}_{3^e}$ if and only if e is odd or $e = 2$ and $a = \pm 1$, see [7, Theorem 3.4]; [10, Proposition 2.1]; and Theorem 4.2 below.

Results from [7] show that composition of a planar polynomial with linearised permutation polynomials results in further planar polynomials, but the resulting planes are all isomorphic. Essentially, Theorem 3.3 connects two seemingly difficult problems: classifying commutative semifields of odd order is equivalent to classifying planar DO polynomials.

We want now to apply the results of Section 2 to Theorem 3.3. In particular, we outline what it means for two planar DO polynomials to generate isotopic presemifields.

Theorem 3.5. *Let $f, h \in \mathbb{F}_q[X]$ be planar DO polynomials and let L, M be linearised permutation polynomials on $\mathbb{F}_q$. There exists an isotopism (M, M, L) between the commutative presemifields $\mathcal{R}_f$ and $\mathcal{R}_h$ if and only if*

$$f(X) \equiv L\big(h\big(M^{-1}(X)\big)\big) \mod \big(X^q - X\big).$$

Proof. If $f(X) \equiv L(h(M^{-1}(X))) \bmod (X^q - X)$, then it is immediate from Theorem 3.3 and [7, Theorem 5.2] that (M, M, L) is an isotopism between $\mathcal{R}_f$ and $\mathcal{R}_h$.

Now suppose there exists an isotopism (M, M, L) between $\mathcal{R}_f$ and $\mathcal{R}_h$. We have

$$\Delta_f\big(M(x), M(y)\big) = L\big(\Delta_h(x, y)\big)$$

for all $x, y \in \mathbb{F}_q$. Equivalently, we have

$$\Delta_f(x, y) = L\big(\Delta_h\big(M^{-1}(x), M^{-1}(y)\big)\big). \tag{1}$$

Using the properties of linearised polynomials, it is easily seen that

$$L\big(\Delta_h\big(M^{-1}(x), M^{-1}(y)\big)\big) = \Delta_{L(h(M^{-1}))}(x, y).$$

For the difference polynomial of a DO polynomial D, we also have $\Delta_D(X, X) = 2D(X)$. Since DO polynomials are closed under composition with linearised polynomials, the combination of these properties in (1) shows $f(X) \equiv L(h(M^{-1}(X))) \bmod (X^q - X)$ as required. □

Theorem 3.6. *Let $q = p^e$ with e odd and suppose $f, h \in \mathbb{F}_q[X]$ are planar DO polynomials. If $\mathcal{R}_f$ and $\mathcal{R}_h$ are isotopic, then there exist linearised permutation polynomials L and M such that $f(X) \equiv L(h(M(X))) \bmod (X^q - X)$.*

This is immediate from Corollary 2.8. Similarly, we have

Theorem 3.7. *Let $f \in \mathbb{F}_q[X]$ be a planar DO polynomial and suppose that $\mathcal{R}_f$ is isotopic to a semifield $\mathcal{R}$ where $\mathcal{N}_m(\mathcal{R}) \subseteq \mathcal{N}_l(\mathcal{R})$. Then every commutative presemifield isotopic to $\mathcal{R}_f$ is of the form $\mathcal{R}_h$ where $h(X) \equiv L(f(M(X))) \bmod (X^q - X)$ for linearised permutation polynomials L and M.*

Theorems 3.6 and 3.7 yield several important corollaries. To begin, we may categorise those planar DO polynomials which describe presemifields isotopic to commutative twisted fields. Let $q = p^e$ and $\alpha \geqslant 1$ satisfy $e/(\alpha, e)$ odd. We have already noted that $f(X) = X^{p^\alpha+1}$ is planar over $\mathbb{F}_q$ in this case and that $\mathcal{R}_f$ is a commutative presemifield (without identity) isotopic to one of the commutative twisted fields of Albert. We may convert $\mathcal{R}_f$ to a semifield by using $a = 1$ in the method given earlier. The resulting commutative semifield, $\mathcal{A}_\alpha$, is the commutative twisted field of Albert with identity 2 generated by the field automorphism X^{p^α}. The following lemma is an application of [3, Theorem 1].

Lemma 3.8. *Let $q = p^e$, $\alpha \geqslant 1$ satisfy $e/(\alpha, e)$ odd and let $\mathcal{A}_\alpha$ denote the commutative twisted field with identity 2 generated by the automorphism X^{p^α}. The left, middle and right nuclei of $\mathcal{A}_\alpha$ are all equal to $\mathbb{F}_{p^d}$ where $d = (\alpha, e)$.*

Since $X^{p^\alpha+1}$ generates a commutative presemifield isotopic to a commutative twisted field, the following corollary is immediate from Theorem 3.7 and the previous lemma.

Corollary 3.9. *Let $f \in \mathbb{F}_q[X]$ be a planar DO polynomial. If $\mathcal{R}_f$ is isotopic to a commutative twisted field, then $f(X) \equiv L(M^{p^\alpha+1}(X)) \bmod (X^q - X)$, where L and M are linearised permutation polynomials and $e/(\alpha, e)$ is odd.*

If $f(X) = \frac{1}{2}X^2$, then $\mathcal{R}_f = \mathbb{F}_q$ for any odd prime power q. Further, $I(f)$ is the Desarguesian plane. Theorem 3.7 can therefore be used to categorise those planar DO polynomials which describe the Desarguesian plane as well.

Corollary 3.10. *Let $f \in \mathbb{F}_q[X]$ be a planar DO polynomial. If $\mathcal{R}_f$ is isotopic to a finite field so that $I(f)$ is the Desarguesian plane, then $f(X) \equiv L(M^2(X)) \bmod (X^q - X)$, where L and M are linearised permutation polynomials.*

This was previously known only for $q = p^2$. Knuth showed in [16] that any semifield of order p^2 is a finite field. Thus Corollary 3.10 completely describes planar DO polynomials over $\mathbb{F}_{p^2}$. Theorem 3.6 allows us to also classify planar DO polynomials over $\mathbb{F}_{p^3}$.

Corollary 3.11. *Let $f \in \mathbb{F}_{p^3}[X]$ be a planar DO polynomial. Then $f(X) \equiv L(M^{p^\alpha+1}(X)) \bmod (X^q - X)$, where L and M are linearised permutation polynomials, and $\alpha \in \{0, 1\}$.*

Proof. In [18], Menichetti showed that a commutative semifield which is three-dimensional over its middle nucleus is necessarily Albert's commutative twisted field. The cases $\alpha = 0$ and $\alpha = 1$ correspond with the finite field case and the twisted field case, respectively. □

At this point in time, we are unable to extend this classification further. For the case $q = p^4$, there are some known examples for general p (and for the specific case $p = 3$) which are neither finite fields nor twisted fields. Certainly, no classification statement comparable to Menichetti's result for $\mathbb{F}_{p^3}$ exists, and the situation does appear to be more complex. For example, Dickson's semifields include examples of order p^4, and these have middle nucleus $\mathbb{F}_{p^2}$ but nucleus $\mathbb{F}_p$. So neither Theorem 3.6 nor Theorem 3.7 can be used for this class.

Let $\mathcal{D}$ be the set of all reduced planar DO polynomials over $\mathbb{F}_q$ and $\mathcal{G}$ the set of all reduced linearised permutation polynomials over $\mathbb{F}_q$. Define the relation R on $\mathcal{D}$ by $(f, h) \in R$ if and only if there exist two linearised permutation polynomials $L, M \in \mathcal{G}$ such that $f(X) \equiv L(h(M(X))) \bmod (X^q - X)$. It is easy to show that R is an equivalence relation. By Theorem 3.5, each equivalence class consists entirely of planar DO polynomials which describe isotopic commutative presemifields, while Theorem 2.6 implies that any commutative presemifield can generate at most two equivalence classes of planar DO polynomials. Recalling that two presemifields coordinatise isomorphic planes if and only if they are isotopic, we summarise with the following statement.

Theorem 3.12. *Let P the set of all equivalence classes described by the relation R defined above. Then the number N_q of non-isomorphic commutative semifield planes of order q satisfies $\frac{1}{2}|P| < N_q \leqslant |P|$, with equality holding if $q = p^e$ with e odd.*

It is clear improving the lower bound in the above theorem requires a better understanding of the second part of Theorem 2.6(ii). In connection with Theorem 2.2(ii), which includes the second part of Theorem 2.6(ii), we may show

Lemma 3.13. *Let $f, h \in \mathbb{F}_q[X]$ be planar DO polynomials and (M, N, L) be an isotopism from $\mathcal{R}_f$ to $\mathcal{R}_h$. If $M(x) \neq N(\alpha x)$ for all $\alpha \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_q^*$, then $\alpha f(N(X)) + \beta L(h(X))$ and $\alpha f(M(X)) + \beta L(h(X))$ are planar DO polynomials over $\mathbb{F}_q$ for all $(\alpha, \beta) \in \mathbb{F}_p \times \mathbb{F}_p \setminus \{(0, 0)\}$.*

Proof. Suppose (M, N, L) is an isotopism from $\mathcal{R}_f$ to $\mathcal{R}_h$ with $M(x) \neq N(\alpha x)$ for all $\alpha \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_q^*$. Set $S(X) \equiv M(N^{-1}(X)) \bmod (X^q - X)$ and $T(X) \equiv N(M^{-1}(X)) \bmod (X^q - X)$. Then $S(X) + \alpha X$ and $T(X) + \alpha X$ are linearised permutation polynomials for all $\alpha \in \mathbb{F}_p$. Now

$$\Delta_f\big(M(x), N(y)\big) = L\big(\Delta_h(x, y)\big)$$

for all $x, y \in \mathbb{F}_q$. Using the definition of the difference polynomial and the properties of linearised polynomials, it can be verified that this is equivalent to

$$\Delta_{f(N)}\big(S(x), y\big) = \Delta_{L(h)}(x, y) = \Delta_{f(M)}\big(T(x), y\big)$$

for all $x, y \in \mathbb{F}_q$. Fix $y \neq 0$. Then we have

$$\Delta_{f(N)}\big(S(X), y\big) \equiv \Delta_{L(h)}(X, y) \mod \big(X^q - X\big)$$

and

$$\Delta_{f(M)}\big(T(X), y\big) \equiv \Delta_{L(h)}(X, y) \mod \big(X^q - X\big).$$

Since $S(X) + \alpha X$ is a permutation polynomial for all $\alpha \in \mathbb{F}_p$, it follows that $\Delta_{f(N)}(S(X) + \alpha X, y)$ is a linearised permutation polynomial also. Now

$$\begin{aligned}
\Delta_{f(N)}\big(S(X) + \alpha X, y\big) &= \Delta_{f(N)}\big(S(X), y\big) + \Delta_{f(N)}(\alpha X, y) \\
&= \Delta_{f(N)}\big(S(X), y\big) + \alpha \Delta_{f(N)}(X, y) \\
&\equiv \Delta_{L(h)}(X, y) + \Delta_{\alpha f(N)}(X, y) \mod \big(X^q - X\big) \\
&\equiv \Delta_{L(h)+\alpha f(N)}(X, y) \mod \big(X^q - X\big).
\end{aligned}$$

It follows that $L(h(X)) + \alpha f(N(X))$ is a planar DO polynomial for all $\alpha \in \mathbb{F}_p$, which is equivalent to our claim. The proof for $L(h(X)) + \alpha f(M(X))$ is essentially the same. □

We note that the conditions on f and h outlined in the above lemma appear to be very restrictive.

4. The known classes of planar DO polynomials

In this final section, we consider the known classes of planar DO polynomials. In particular, we resolve the isotopy problem for the class of DO polynomials $X^{10} + aX^6 - a^2X^2$. We first consider the commutative twisted fields of Albert.

As already mentioned, the monomial $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd. In such cases the presemifield defined by $X^{p^\alpha+1}$ is isotopic to the twisted field of Albert with $c = -1$, [1]. In fact, $c = -1$ is the only commutative class generated by Albert's generalised twisted fields, see [3, Theorem 2]. In the remainder we denote the commutative presemifield defined by $X^{p^\alpha+1}$ by $\mathcal{A}_\alpha$ (although this differs slightly from our earlier notation, we feel it should not cause confusion). Rather than appealing to the results of Albert, we use the theory developed in this article to establish when commutative twisted fields are distinct from a finite field.

Theorem 4.1. *Suppose $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$. Then $\mathcal{A}_\alpha$ is isotopic to a finite field if and only if $\alpha \equiv 0 \bmod e$.*

Proof. Set $q = p^e$. By Corollary 3.10, $\mathcal{A}_\alpha$ is isotopic to $\mathbb{F}_q$ if and only if $X^{p^\alpha+1} \equiv L'(M^2(X)) \bmod (X^q - X)$ where L' and M are linearised permutation polynomials over $\mathbb{F}_q$. Equivalently, $\mathcal{A}_\alpha$ is isotopic to $\mathbb{F}_q$ if and only if there exist linearised permutation polynomials L, M over $\mathbb{F}_q$ such that $L(X^{p^\alpha+1}) \equiv M^2(X) \bmod (X^q - X)$. If $\alpha \equiv 0 \bmod e$, then $X^{p^\alpha+1} \equiv X^2 \bmod (X^q - X)$ and so in this case $X^{p^\alpha+1}$ describes a presemifield isotopic to $\mathbb{F}_q$. Now suppose $\alpha \not\equiv 0 \bmod e$. Set $L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}$ and $M(X) = \sum_{i=0}^{e-1} b_i X^{p^i}$. We have

$$L\left(X^{p^\alpha+1}\right) = \sum_{i=0}^{e-1} a_i X^{p^{\alpha+i}+p^i}$$

and

$$M(X)^2 = \sum_{i,j=0}^{e-1} b_i b_j X^{p^i+p^j}.$$

Working modulo $X^q - X$ is equivalent to working with the exponents i and j (in $X^{p^i+p^j}$) modulo e. For ease of notation, we work with the subscripts of coefficients modulo e also. Equating $X^{p^t+p^t}$ terms in the equation $L(X^{p^\alpha+1}) \equiv M^2(X) \bmod (X^q - X)$ we obtain $b_t^2 = 0$, implying $b_t = 0$ for all $t \in \{0, \ldots, e-1\}$. So $M(X) = 0$, contradicting the permutation behaviour of M. Hence $\mathcal{A}_\alpha$ is not isotopic to $\mathbb{F}_q$ when $\alpha \not\equiv 0 \bmod e$. □

We now move on to consider the presemifields generated by the planar DO polynomials $g_5(X^2, a) = X^{10} + aX^6 - a^2X^2$ where $g_5(X, a)$ is the Dickson polynomial of the first kind of degree five. The monograph [17] deals solely with the Dickson polynomials of the first and second kind.

Theorem 4.2. *For any non-zero $a \in \mathbb{F}_{3^e}$, the polynomial $g_5(X^2, a) = X^{10} + aX^6 - a^2X^2$ is a planar DO polynomial over $\mathbb{F}_{3^e}$ if and only if either e is odd or $e = 2$ and $a = \pm 1$. Further, for non-zero $a, b \in \mathbb{F}_{3^e}$ and $e \geqslant 3$ odd, $g_5(X^2, a)$ and $g_5(X^2, b)$ generate isotopic presemifields whenever*

(i) *a and b are both squares in $\mathbb{F}_{3^e}$,*
(ii) *a and b are both non-squares in $\mathbb{F}_{3^e}$.*

Proof. For $e = 1$, $g_5(X^2, a) \equiv (1 + a - a^2)X^2 \bmod (X^3 - X)$ which is clearly planar as $1 + a - a^2 \neq 0$ for all $a \in \mathbb{F}_3$. For $e = 2$, $g_5(X^2, a) \equiv aX^6 + (1 - a^2)X^2 \bmod (X^3 - X)$. Put $G(X) = aX^6 + (1 - a^2)X^2$. When $a = \pm 1$, $G(X) = \pm X^6 = \pm(X^2)^3$, which is planar. For $a \neq \pm 1$, it is easily checked that $G(X) = aX^6 + (1 - a^2)X^2$ is not planar over $\mathbb{F}_9$.

Suppose $e \geqslant 3$. Lemma 2.6(ii) of [17] states

$$b^k g_k(X, a) = g_k\left(bX, b^2 a\right) \tag{2}$$

for $b \in \mathbb{F}_q$. From [7], $g_5(X^2, 1) = X^{10} + X^6 - X^2$ is a planar DO polynomial over $\mathbb{F}_{3^e}$ if and only if e is odd. Therefore it follows from (2) that this is true for all DO polynomials $g_5(X^2, a)$ where $a \in \mathbb{F}_{3^e}$ is a square. Using similar arguments to those of [7] for $g_5(X^2, 1)$, $g_5(X^2, -1) = X^{10} - X^6 - X^2$ is shown to be planar if and only if e is odd. Using (2) extends this result to the polynomials $g_5(X^2, a)$ where $a \in \mathbb{F}_{3^e}$ is a non-square.

Now let $L(X) = b^{2k}X$ and $M(X) = bX$ where $b \in \mathbb{F}_q^*$. The polynomials L and M are obviously linearised permutation polynomials over $\mathbb{F}_q$. Using (2) we have

$$L\big(g_k\big(X^2, a\big)\big) = b^{2k} g_k\big(X^2, a\big) = g_k\big((bX)^2, b^4 a\big)$$

and

$$g_k\big(M^2(X), b^4 a\big) = g_k\big((bX)^2, b^4 a\big).$$

In this case we have $f(X) = g_k(X^2, a)$ is isotopic to $h(X) = g_k(X^2, b^4 a)$. As $\gcd(4, 3^e - 1) = 2$ (because $e \geqslant 3$ is odd), then $\{b^4 \mid b \in \mathbb{F}_{3^e}\}$ is exactly the set of all squares in $\mathbb{F}_{3^e}$. The remaining statements now follow. □

Note that the planarity of $g_5(X^2, a)$ over $\mathbb{F}_q$ for e odd has been established in [10]. From the above theorem, the question of isotopy for the presemifields generated using the polynomials $g_5(X^2, a) \in \mathbb{F}_{3^e}[X]$ reduces to the question of isotopy for the presemifields $\mathcal{R}_f$ and $\mathcal{R}_h$ where $f(X) = X^{10} + X^6 - X^2$ and $h(X) = X^{10} - X^6 - X^2$. Among the known classes of commutative semifields of odd order, finite fields and Albert's commutative twisted fields yield the only examples with order p^e where e is odd. Thus, to determine when $\mathcal{R}_f$ and $\mathcal{R}_h$ are distinct from the known classes, we need only determine when they are distinct from these two classes (ignoring the case where $e = 2$). We proceed now to do precisely this. We shall deal first with the finite field case which includes the case $e = 2$.

Theorem 4.3. *Let $f(X) = X^{10} + X^6 - X^2$ and $h(X) = X^{10} - X^6 - X^2$ be planar polynomials over $\mathbb{F}_{3^e}$.*

(i) *$\mathcal{R}_f$ is isotopic to the finite field $\mathbb{F}_{3^e}$ if and only if $e \in \{1, 2\}$.*
(ii) *$\mathcal{R}_h$ is isotopic to the finite field $\mathbb{F}_{3^e}$ if and only if $e \in \{1, 2, 3\}$.*

Proof. Set $q = 3^e$. If $e = 1$, then $X^{10} \pm X^6 - X^2 \equiv \pm X^2 \bmod (X^q - X)$, and so both are isotopic to $\mathbb{F}_q$. If $e = 2$, then $X^{10} \pm X^6 - X^2 \equiv \pm X^6 \bmod (X^q - X)$. As $X^6 = (X^2)^p$, both must again be isotopic to $\mathbb{F}_q$ by Corollary 3.10. For $e > 2$, $f(X)$ and $h(X)$ are planar provided e is odd.

For $e = 3$, $\mathcal{R}_h$ is isotopic to $\mathbb{F}_q$: the triple $(M^{-1}(X), M^{-1}(X), L(X))$ is a strong isotopism between $\mathcal{R}_h$ and $\mathbb{F}_q$, where

$$L(X) = \big(\alpha^2 - \alpha - 1\big)X^9 - \alpha X^3 - \big(\alpha^2 - \alpha\big)X,$$
$$M(X) = \big(\alpha^2 - \alpha\big)X^9 + \alpha X^3 + X$$

and α is a solution of the equation $y^3 - y - 1 = 0$.

We now consider specifically $\mathcal{R}_f$. Similar arguments can be used for $\mathcal{R}_h$. Suppose $\mathcal{R}_f$ is isotopic to $\mathbb{F}_q$. By Corollary 3.10, there exist linearised permutation polynomials L, M such that

$$L\big(f(X)\big) \equiv M(X)^2 \mod \big(X^q - X\big).$$

Set $L(X) = \sum_{i=0}^{e-1} a_i X^{3^i}$ and $M(X) = \sum_{i=0}^{e-1} b_i X^{3^i}$. We have

$$\sum_{i=0}^{e-1} a_i \big(X^{3^{i+2}+3^i} + X^{3^{i+1}+3^{i+1}} - X^{3^i+3^i}\big) \equiv \sum_{i,j=0}^{e-1} b_i b_j X^{3^i+3^j} \mod \big(X^q - X\big). \tag{3}$$

Suppose $e \geqslant 5$. Equating coefficients in the reduced forms of each side of (3), we obtain the set of equations

$$a_i = 2b_i b_{i+2}, \tag{4}$$

$$0 = 2b_i b_{i+1}, \tag{5}$$

$$a_{i-1} - a_i = b_i^2 \tag{6}$$

for $0 \leqslant i \leqslant e-1$ and where the subscripts are taken modulo e (here (4) corresponds to $X^{3^{i+2}+3^i}$, (5) to $X^{3^{i+1}+3^i}$, and (6) to $X^{3^i+3^i}$). From (5), there are two cases: either $b_i = b_{i+1} = 0$, or $b_i \neq 0$ and $b_{i-1} = b_{i+1} = 0$. In the first case, combining (4) with (6) we get $a_{i-1} = a_i = a_{i+1} = 0$. In the second case, from (6) $a_i = a_{i+1}$, while using (4) we obtain $a_{i-1} = a_{i+1} = 0$. In either case, we have $a_{i-1} = a_i = a_{i+1} = 0$. Since this holds for each i, it follows that $a_i = 0$ for all i. Hence $L(X) = 0$, contradicting the permutation behaviour of L. Therefore $\mathcal{R}_f$ is not isotopic to $\mathbb{F}_q$ for all odd $e \geqslant 5$.

It remains to deal with the case $e = 3$ for $\mathcal{R}_f$. Equating coefficients in the reduced forms of each side of (3) again, we obtain

$$a_0 - a_1 = b_1^2, \tag{7}$$

$$a_1 - a_2 = b_2^2, \tag{8}$$

$$a_2 - a_0 = b_0^2, \tag{9}$$

$$a_0 = 2b_2 b_0, \tag{10}$$

$$a_1 = 2b_0 b_1, \tag{11}$$

$$a_2 = 2b_1 b_2. \tag{12}$$

Suppose $b_i = 0$ for some $i \in \{0, 1, 2\}$. Assume $b_0 = 0$. By (10) and (11), $a_0 = a_1 = 0$ and so from (7), $b_1^2 = 0$. But now $a_2 = 0$ from (12), implying $L(X) = 0$, a contradiction. Similarly, $b_1 \neq 0$ and $b_2 \neq 0$. Hence $b_i \neq 0$ for all $i \in \{0, 1, 2\}$. Subtracting (9) from (12) yields

$$a_0 = 2b_1 b_2 + 2b_0^2. \tag{13}$$

Similar combinations yield

$$a_1 = 2b_2b_0 + 2b_1^2, \tag{14}$$

$$a_2 = 2b_0b_1 + 2b_2^2. \tag{15}$$

If $b_0 = b_1$, then $a_1 = 2b_1^2$ from (11). Now (14) shows $2b_2b_0 = 0$, contradicting $b_i \neq 0$ for all i. So $b_0 \neq b_1$. Again, similar arguments show $b_0 \neq b_2$ and $b_1 \neq b_2$.

Put $b_1 = \alpha b_0$ and $b_2 = \beta b_0$ with $\alpha, \beta \notin \{0, 1\}$ and $\alpha \neq \beta$. Combining (10) with (13), (11) with (14), and (12) with (15), we obtain the set of equations

$$\alpha\beta + 1 = \beta,$$
$$\beta + \alpha^2 = \alpha,$$
$$\alpha + \beta^2 = \alpha\beta.$$

It is now easy to show this system has no solution in $\mathbb{F}_{27}$. As there are no remaining possibilities, we conclude $\mathcal{R}_f$ is not isotopic to $\mathbb{F}_q$ when $e = 3$. □

It remains to compare $\mathcal{R}_f$ and $\mathcal{R}_h$ with Albert's commutative twisted fields. Since any commutative twisted field of order p or p^2 is necessarily strongly isotopic to a finite field, we consider only the situation for commutative twisted fields of order 3^e with $e \geqslant 3$.

Theorem 4.4. *Let $e \geqslant 3$ be odd so that $X^{p^\alpha+1}$, $f(X) = X^{10} + X^6 - X^2$ and $h(X) = X^{10} - X^6 - X^2$ are planar polynomials over $\mathbb{F}_{3^e}$. Denote the corresponding commutative presemifields by $\mathcal{A}_\alpha, \mathcal{R}_f$ and $\mathcal{R}_h$, respectively.*

(i) *$\mathcal{R}_f$ and $\mathcal{A}_\alpha$ are isotopic if and only if $e = 3$ and $\alpha \not\equiv 0 \bmod e$.*
(ii) *$\mathcal{R}_h$ and $\mathcal{A}_\alpha$ are isotopic if and only if $e = 3$ and $\alpha \equiv 0 \bmod e$.*

Proof. Set $q = 3^e$.

If $\alpha \equiv 0 \bmod e$, then $\mathcal{A}_\alpha$ is isotopic to $\mathbb{F}_q$ by Theorem 4.1. Now Theorem 4.3 shows $\mathcal{R}_h$ is isotopic to $\mathcal{A}_\alpha$ if and only if $e = 3$, while $\mathcal{R}_f$ is never isotopic to $\mathcal{A}_\alpha$. If $\alpha \not\equiv 0 \bmod e$ and $e = 3$, then $\mathcal{R}_f$ is commutative and 3-dimensional over $\mathbb{F}_3$. By the result of Menichetti, [18], $\mathcal{R}_f$ must be isotopic to $\mathcal{A}_\alpha$.

Now let $e \geqslant 5$ be odd. We again deal with $\mathcal{R}_f$ only as similar arguments can be used for $\mathcal{R}_h$. Suppose $\mathcal{R}_f$ and $\mathcal{A}_\alpha$ describe isotopic presemifields. Throughout we assume $0 < \alpha < e/2$ as Corollary 3.9 shows $X^{p^\alpha+1}$ and $X^{p^{e-\alpha}+1}$ yield isotopic presemifields. First consider the case $\alpha > 1$. By Corollary 3.9 there exist linearised permutation polynomials L and M over $\mathbb{F}_q$ such that

$$L\big(X^{3^\alpha+1}\big) \equiv M(X)^{10} + M(X)^6 - M(X)^2 \mod \big(X^q - X\big).$$

Set $L(X) = \sum_{i=0}^{e-1} a_i X^{3^i}$ and $M(X) = \sum_{i=0}^{e-1} b_i X^{3^i}$. We have

$$L\big(X^{3^\alpha+1}\big) = \sum_{i=0}^{e-1} a_i X^{3^{\alpha+i}+3^i}$$

and

$$M(X)^{10} + M(X)^6 - M(X)^2 = \sum_{i,j=0}^{e-1} b_i^9 b_j X^{3^{i+2}+3^j} + b_i^3 b_j^3 X^{3^{i+1}+3^{j+1}} - b_i b_j X^{3^i+3^j}.$$

Again we proceed by equating the coefficients in the reduced form of each polynomial, retaining the convention of considering subscripts modulo e. Equating coefficients of terms of the form $X^{3^i+3^i}$ yields the equation

$$0 = b_{i-2}^9 b_i + b_{i-1}^6 - b_i^2. \tag{16}$$

If $b_i = 0$ for any i, then (16) implies $b_{i-1} = 0$ also. It follows that $b_i = 0$ for all i, in which case $M(X) = 0$, contradicting the permutation behaviour of M. Consequently, $b_i \neq 0$ for all $i \in \{0, \ldots, e-1\}$. We rewrite (16) to get

$$b_{i-2}^9 = b_i - \frac{b_{i-1}^6}{b_i}. \tag{17}$$

Dividing by b_{i-1}^3 gives the identity

$$\left(\frac{b_{i-2}^3}{b_{i-1}}\right)^3 = \frac{b_i}{b_{i-1}^3} - \frac{b_{i-1}^3}{b_i}. \tag{18}$$

As $\alpha > 1$, equating coefficients of terms of the form $X^{3^{i+1}+3^i}$ we obtain

$$0 = b_{i-1}^9 b_i + b_{i-2}^9 b_{i+1} - b_{i-1}^3 b_i^3 + b_i b_{i+1} \tag{19}$$

(where we have used the fact we are in characteristic 3). Using (17) we obtain

$$\begin{aligned} 0 &= \left(b_{i+1} - \frac{b_i^6}{b_{i+1}}\right) b_i + \left(b_i - \frac{b_{i-1}^6}{b_i}\right) b_{i+1} - b_{i-1}^3 b_i^3 + b_i b_{i+1} \\ &= -\frac{b_i^7}{b_{i+1}} - \frac{b_{i-1}^6 b_{i+1}}{b_i} - b_{i-1}^3 b_i^3, \end{aligned}$$

and multiplying through by $b_i b_{i+1}$ yields

$$\begin{aligned} 0 &= b_i^8 + b_{i-1}^6 b_{i+1}^2 + b_i^4 b_{i+1} b_{i-1}^3 \\ &= b_i^4 \left(b_i^4 - b_{i+1} b_{i-1}^3\right) + b_{i-1}^3 b_{i+1} \left(b_{i-1}^3 b_{i+1} - b_i^4\right) \\ &= \left(b_i^4 - b_{i-1}^3 b_{i+1}\right)^2. \end{aligned}$$

Hence $b_i^4 = b_{i-1}^3 b_{i+1}$ holds for all i. Equivalently, we have

$$\frac{b_i^3}{b_{i+1}} = \frac{b_{i-1}^3}{b_i} \tag{20}$$

for all i. Returning to (18) and setting $t = b_{i-1}^3/b_i$, we have $t^4 + t^2 - 1 = 0$. Now $x^2 + x - 1 = 0$ only has solutions in even extensions of $\mathbb{F}_3$ and so no such t exists. It follows that there are no linearised permutation polynomials L and M satisfying our assumption. So for $\alpha > 1$, $\mathcal{R}_f$ and $\mathcal{A}_\alpha$ are not isotopic.

It remains to deal with the case $\alpha = 1$ and $e \geqslant 5$. Suppose $\mathcal{R}_f$ and $\mathcal{A}_\alpha$ describe isotopic presemifields. Again we appeal to Corollary 3.9 so that $L(h(X)) \equiv f(M(X)) \bmod (X^q - X)$ (note that our application of Corollary 3.9 is slightly different to the previous case; we have interchanged f and h). Set $L(X) = \sum_{i=0}^{e-1} a_i X^{3^i}$ and $M(X) = \sum_{i=0}^{e-1} b_i X^{3^i}$. Equating coefficients of the $X^{3^{i+1}+3^i}$ terms, we obtain the equation

$$0 = b_i^4 + b_{i+1} b_{i-1}^3. \tag{21}$$

Suppose that $b_i \neq 0$ for all i. Then we have the identity

$$\frac{b_i}{b_{i-1}^3} = -\frac{b_{i+1}}{b_i^3}.$$

We may extend this to obtain the equation

$$\frac{b_i}{b_{i-1}^3} = (-1)^k \frac{b_{i+k}}{b_{i+k-1}^3}.$$

As we may work with subscripts modulo e, setting $k = e$ we have

$$\frac{b_i}{b_{i-1}^3} = -\frac{b_i}{b_{i-1}^3}$$

since e is odd. But this implies $b_i = 0$, contradicting our assumption that $b_i \neq 0$ for all i. Hence there must be some t for which $b_t = 0$. Returning to (21), it is immediate that $b_{t-1}^4 = 0$, and so $b_{t-1} = 0$. Inductively, we have $b_i = 0$ for all i which proves $M(X) = 0$, again contradicting the permutation behaviour of M. Hence $\mathcal{R}_f$ and $\mathcal{A}_\alpha$ are not isotopic presemifields when $\alpha = 1$ and $e \geqslant 5$. □

It follows from our previous two results, that $f(X) = X^{10} + X^6 - X^2$ and $h(X) = X^{10} - X^6 - X^2$ generate presemifields not isotopic to any known presemifield for each odd $e \geqslant 5$. We now complete our considerations by determining when f and h generate isotopic presemifields.

Theorem 4.5. *Let $f(X) = X^{10} + X^6 - X^2$ and $h(X) = X^{10} - X^6 - X^2$ be planar polynomials over $\mathbb{F}_q$ where $q = 3^e$. Then $\mathcal{R}_f$ and $\mathcal{R}_h$ are isotopic if and only if $e = 1, 2$.*

Proof. The cases $e = 1, 2, 3$ follow immediately from Theorem 4.3. Assume $e \geqslant 5$. To complete the proof it follows from Corollary 2.8 and Theorem 3.5 that we need only show that for $e \geqslant 5$ there exist no linearised permutation polynomials $L, M \in \mathbb{F}_q$ satisfying

$$L\big(f(X)\big) \equiv h\big(M(X)\big) \mod \big(X^q - X\big). \tag{22}$$

To the contrary, suppose there exist linearised permutation polynomials $L, M \in \mathbb{F}_q[X]$ satisfying (22). Put

$$L(X) = \sum_{i=0}^{e-1} a_i X^{3^i} \quad \text{and} \quad M(X) = \sum_{i=0}^{e-1} b_i X^{3^i}.$$

Now

$$L\big(f(X)\big) = \sum_{i=0}^{e-1} \big(a_i X^{3^{i+2}+3^i} + a_i X^{3^{i+1}+3^{i+1}} - a_i X^{3^i+3^i}\big)$$

and

$$h\big(M(X)\big) = \sum_{i,j=0}^{e-1} \big(b_i^9 b_j X^{3^{i+2}+3^j} - b_i^3 b_j^3 X^{3^{i+1}+3^{j+1}} - b_i b_j X^{3^i+3^j}\big).$$

Now we equate the coefficients of the corresponding terms of $L(f(X))$ and $h(M(X))$, considering all subscripts modulo e. Equating coefficients of the terms of degree $3^{i+2}+3^i$ and 3^i+3^i we have

$$a_\alpha = b_\alpha^{10} + b_{\alpha-2}^9 b_{\alpha+2} + b_{\alpha-1}^3 b_{\alpha+1}^3 + b_\alpha b_{\alpha+2} \tag{23}$$

and

$$a_{\alpha-1} - a_\alpha = b_{\alpha-2}^9 b_\alpha - b_{\alpha-1}^6 - b_\alpha^2, \tag{24}$$

respectively, for $\alpha \in \{0, 1, \ldots, e-1\}$. All other equations are given by equating the coefficients of the terms of degree $3^{i+t}+3^i$ with $t \in \{1, 3, 4, 5, \ldots, (e-1)/2\}$ (as otherwise the terms reduce):

$$0 = b_{\alpha+t-2}^9 b_\alpha + b_{\alpha-2}^9 b_{\alpha+t} + b_{\alpha+t-1}^3 b_{\alpha-1}^3 + b_{\alpha+t} b_\alpha \tag{25}$$

where again $\alpha \in \{0, 1, \ldots, e-1\}$.

Assume that $e \geqslant 7$ (we will deal separately with the case $e = 5$ below). We first show that none of the coefficients of M can be zero. As M permutes $\mathbb{F}_q$, not all of its coefficients can be zero. Suppose s is an integer satisfying $b_s = 0$ and $b_{s-1} \neq 0$. We will show that $b_{s+1} = 0$ and $b_{s+2} = 0$ (in other words that we have three consecutive coefficients that are zero).

From (25) with $t = 1$ and $\alpha = s-1$

$$b_{s-2}^9 b_{s-1} + b_{s-1}^3 b_{s-2}^3 = 0.$$

Dividing by b_{s-1}^4 gives

$$\left(\frac{b_{s-2}^3}{b_{s-1}}\right)^3 + \frac{b_{s-2}^3}{b_{s-1}} = 0.$$

In other words, $b_{s-2}^3/b_{s-1} \in \mathbb{F}_{3^e}$ is a root of $X^3 + X = X(X^2+1)$. It follows that $b_{s-2} = 0$ (because -1 is a non-square in $\mathbb{F}_{3^e}$ for odd e). So, if $b_s = 0$ and $b_{s-1} \neq 0$, we must have $b_{s-2} = 0$.

From (25) with $t = 3$ and $\alpha = s$ we have $b_{s+2}^3 b_{s-1}^3 = 0$, so $b_{s+2} = 0$. Also from (25) with $t = 1$ and $\alpha = s-2$ we have $b_{s-1}^3 b_{s-4}^3 = 0$, so $b_{s-4} = 0$. As $b_{s+2} = b_s = b_{s-2} = b_{s-4} = 0$, then from (25) with $t = 3$ and $\alpha = s-4$ we have $b_{s-6}^9 b_{s-1} = 0$, so $b_{s-6} = 0$. So if $b_s = 0$ and $b_{s-1} \neq 0$, then we have $b_{s+2} = b_{s-2} = b_{s-4} = b_{s-6} = 0$. If $e = 7$, as $b_{s+1} = b_{s-6}$ it follows $b_{s+1} = 0$ and we have for this case that $b_s = b_{s+1} = b_{s+2} = 0$.

Suppose $e > 7$. We may consider (25) with $t = 4$ and $\alpha = s$: that is $0 = b_{s+3}^3 b_{s-1}^3$, which implies $b_{s+3} = 0$. Now in (23) with $\alpha = s+1, s+2$ we have, respectively, $a_{s+1} = b_{s+1}^{10}$ and $a_{s+2} = 0$, giving $a_{s+1} - a_{s+2} = b_{s+1}^{10}$. On the other hand, (24) with $\alpha = s+2$ gives $a_{s+1} - a_{s+2} = -b_{s+1}^6$. Thus we have $b_{s+1}^{10} = -b_{s+1}^6$. It follows that $b_{s+1} = 0$ (again as -1 is a non-square in $\mathbb{F}_{3^e}$). Again we have $b_s = b_{s+1} = b_{s+2} = 0$.

Now, using the fact that $b_s = b_{s+1} = b_{s+2} = 0$ for $e \geqslant 7$, from (23) with $\alpha = s-1$ we have $a_{s-1} = b_{s-1}^{10}$, while from (23) with $\alpha = s$ we have $a_s = 0$. So $a_{s-1} - a_s = b_{s-1}^{10}$. On the other hand, (24) with $\alpha = s$ gives $a_{s-1} - a_s = -b_{s-1}^6$. So we have $b_{s-1}^{10} = -b_{s-1}^6$, or, as $b_{s-1} \neq 0$, $b_{s-1}^4 = -1$. As $y^4 + 1$ has no roots in odd extensions of $\mathbb{F}_3$, we have a contradiction. So for $e \geqslant 7$, all of the coefficients of M are non-zero.

As all of the coefficients of M are non-zero, we can proceed to re-arrange (25) to obtain:

$$\left(\frac{b_{\alpha+t-2}^3}{b_{\alpha+t-1}}\right)^3 \left(\frac{b_a}{b_{\alpha-1}^3}\right) + \left(\frac{b_{\alpha-2}^3}{b_{\alpha-1}}\right)^3 \left(\frac{b_{\alpha+t}}{b_{\alpha+t-1}^3}\right) + \left(\frac{b_{\alpha+t}}{b_{\alpha+t-1}^3}\right)\left(\frac{b_\alpha}{b_{\alpha-1}^3}\right) + 1 = 0.$$

Putting $x_s = b_s^3/b_{s+1}$ for each integer $s \in \{0, \ldots, e-1\}$ we obtain

$$\begin{aligned} 0 &= \left(x_{\alpha+t-2}^3 - x_{\alpha+t-1}^{-1}\right)x_{\alpha-1}^{-1} + \left(x_{\alpha-2}^3 - x_{\alpha-1}^{-1}\right)x_{\alpha+t-1}^{-1} + 1 \\ &= x_{\alpha+t-2}^3 x_{\alpha+t-1} + x_{\alpha-2}^3 x_{\alpha-1} + x_{\alpha-1}x_{\alpha+t-1} + 1 \end{aligned}$$

which holds for $t \in \{1, 3, 4, \ldots, (e-1)/2\}$. From the above equation, we can generate a new set of equations. For $t = 1$ with $\alpha = s$ and $\alpha = s+1$, respectively, we have

$$0 = x_{s-1}^3 x_s + x_{s-2}^3 x_{s-1} + x_{s-1}x_s + 1, \tag{26}$$

$$0 = x_s^3 x_{s+1} + x_{s-1}^3 x_s + x_s x_{s+1} + 1. \tag{27}$$

For $t = 3$ with $\alpha = s-2$ and $\alpha = s+1$, respectively, we have

$$0 = x_{s-1}^3 x_s + x_{s-4}^3 x_{s-3} + x_{s-3}x_s + 1,$$

$$0 = x_{s+1}^3 x_{s+3} + x_{s-1}^3 x_s + x_s x_{s+3} + 1.$$

Rearranging these four equations gives

$$-\left(1 + x_{s-1}^3 x_s\right) = x_{s-2}^3 x_{s-1} + x_{s-1}x_s \tag{28}$$

$$= x_s^3 x_{s+1} + x_s x_{s+1} \tag{29}$$

$$= x_{s-4}^3 x_{s-3} + x_{s-3} x_s \tag{30}$$

$$= x_{s+1}^3 x_{s+3} + x_s x_{s+3}. \tag{31}$$

Using the right-hand side of (28) and (29) with $s = r+2$, (30) and (28) with $s = r+4$, and (28) and (31) with $s = r$, in turn gives

$$x_r^3 x_{r+1} + x_{r+1} x_{r+2} = x_{t+2}^3 x_{r+3} + x_{r+2} x_{r+3}, \tag{32}$$

$$x_r^3 x_{r+1} + x_{r+1} x_{r+4} = x_{t+2}^3 x_{r+3} + x_{r+3} x_{r+4}, \tag{33}$$

$$x_r^3 x_{r+1} + x_r x_{r+1} = x_{t+2}^3 x_{r+3} + x_r x_{r+3}. \tag{34}$$

From (32) subtract (33), (33) subtract (34), and (34) subtract (32), obtaining respectively,

$$0 = (x_{r+1} - x_{r+3})(x_{r+2} - x_{r+4}),$$

$$0 = (x_{r+1} - x_{r+3})(x_{r+4} - x_r),$$

$$0 = (x_{r+1} - x_{r+3})(x_r - x_{r+2}).$$

Therefore, for each $r \in \{0, 1, \ldots, e-1\}$ we have $x_{r+1} = x_{r+3}$ or $x_r = x_{r+2} = x_{r+4}$. Relabelling we have $x_{r-1} = x_{r+1}$ or $x_{r-2} = x_r = x_{r+2}$. Suppose $x_{r-2} = x_r = x_{r+2}$. Returning to (26) and (27) with $s = r$ we have

$$0 = x_{r-1}^3 x_r + x_r^3 x_{r-1} + x_{r-1} x_r + 1, \tag{35}$$

$$0 = x_r^3 x_{r+1} + x_{r-1}^3 x_r + x_r x_{r+1} + 1. \tag{36}$$

Now subtracting (36) from (35) gives

$$\begin{aligned} 0 &= x_r^3 (x_{r-1} - x_{r+1}) + x_r (x_{r-1} - x_{r+1}) \\ &= x_r \left(x_r^2 + 1\right)(x_{r-1} - x_{r+1}). \end{aligned}$$

As $x_r \neq 0$ for any r and $y^2 + 1$ is irreducible over odd extensions of $\mathbb{F}_3$, we must have $x_{r-1} = x_{r+1}$.

So overall $x_{r-1} = x_{r+1}$ for all $r \in \{0, 1, \ldots, e-1\}$. As e is odd, cycling through the x_i, we have $x_r = x_{r+1}$ for all $0 \leqslant r \leqslant e-1$. Now, finally, (26) gives a contradiction: there are no solutions x_r to $x_r^4 - x_r^2 - 1 = 0$ in $\mathbb{F}_{3^e}$ when e is odd as $y^4 - y^2 - 1$ has no roots in odd extensions of $\mathbb{F}_3$. It follows that for $e \geqslant 7$ there are no linearised permutation polynomials satisfying (22).

It still remains to deal with the case where $e = 5$. The equations for this case are (23), (24) and the specific case of (25) with $t = 1$:

$$0 = b_{\alpha-1}^9 b_\alpha + b_{\alpha-2}^9 b_{\alpha+1} + b_\alpha^3 b_{\alpha-1}^3 + b_{\alpha+1} b_\alpha \tag{37}$$

(other values for t do not give rise to distinct equations). Suppose that $b_s = 0$ for some $s \in \{0, 1, 2, 3, 4\}$. We show that if one coefficient is zero, then there must be at least three consecutive coefficients that are zero. This then leads to a contradiction.

From (37) with $\alpha = s$ we have $0 = b_{s-2}^9 b_{s+1}$. So $b_{s-2} = 0$ or $b_{s+1} = 0$. If $b_{s+1} = 0$, then using $\alpha = s+1$ in (37) we have $b_{s-1}b_{s+2} = 0$. At least one of b_{s-1}, b_{s+2} must be zero. Either of these cases gives three consecutive zero coefficients. Now suppose that $b_{s+1} \neq 0$ which implies $b_{s-2} = 0$. From (37) with $\alpha = s-2$, $b_{s-4}^9 b_{s-1} = 0$. As $b_{s-4} = b_{s+1} \neq 0$ we have $b_{s-1} = 0$. So in all cases we obtain three consecutive coefficients that are zero.

We now have three consecutive zero coefficients, that is $b_r = b_{r+1} = b_{r+2}$ for some integer r. From (37) with $\alpha = r+3$ we have $b_{r+3}b_{r+4} = 0$. Only one of b_{r+3}, b_{r+4} can be zero as otherwise M is the zero polynomial, which contradicts that M is a permutation polynomial over $\mathbb{F}_q$. In either case we have from (23) that $a_{r+t} = b_{r+t}^{10}$ while $a_{r+t+1} = 0$ for $t = 3, 4$. So in (24) we have $a_{r+t} - a_{r+t+1} = a_{r+t} = -b_{r+t}^6$. It follows that $b_{r+t}^{10} = -b_{r+t}^6$ which we have already seen has no solutions other than $b_{r+t} = 0$. So $b_{r+3} = 0$, implies $b_{r+4} = 0$ and vice-versa. Therefore we have shown that if any of the coefficients of M are zero, then M is the zero polynomial, a contradiction.

As the b_i, for $i \in \{0, 1, 2, 3, 4\}$, are non-zero, we have (in the same way as before) the equations

$$0 = x_\alpha^3 x_{\alpha+1} + x_{\alpha-1}^3 x_\alpha + x_\alpha x_{\alpha+1} + 1$$

for $\alpha \in \{0, 1, 2, 3, 4\}$. It is quickly checked, using an algebra package such as MAGMA [4], that there are no solutions to these equations over $\mathbb{F}_{3^5}$ (this can in fact be shown using only four of the equations). Thus it follows that when $e = 5$ there are no solutions to (22). □

Combining the results of this section we have the following corollary.

Corollary 4.6. *The class of planar DO polynomials* $\{g_5(X^2, a) \mid a \in \mathbb{F}_q^*\}$ *generates exactly two non-isomorphic commutative semifield planes for each odd* $e \geqslant 3$. *These are new for all odd* $e \geqslant 5$.

References

[1] A.A. Albert, On nonassociative division algebras, Trans. Amer. Math. Soc. 72 (1952) 296–309.
[2] A.A. Albert, Finite division algebras and finite planes, in: Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics, Providence, in: Symposia in Appl. Math., vol. 10, American Mathematical Society, 1960, pp. 53–70.
[3] A.A. Albert, Generalized twisted fields, Pacific J. Math. 11 (1961) 1–8.
[4] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265.
[5] S.D. Cohen, M.J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, J. Algebra 75 (1982) 373–385.
[6] R.S. Coulter, The classification of planar monomials over fields of prime square order, Proc. Amer. Math. Soc. 134 (2006) 3373–3378.
[7] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.
[8] P. Dembowski, T.G. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 103 (1968) 239–258.
[9] L.E. Dickson, On commutative linear algebras in which division is always uniquely possible, Trans. Amer. Math. Soc. 7 (1906) 514–522.
[10] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory. Ser. A 113 (2006) 1526–1535.
[11] M.J. Ganley, Central weak nucleus semifields, European J. Combin. 2 (1981) 339–347.
[12] D. Gluck, A note on permutation polynomials and finite geometries, Discrete Math. 80 (1990) 97–100.
[13] Y. Hiramine, A conjecture on affine planes of prime order, J. Combin. Theory Ser. A 52 (1989) 44–50.

[14] Y. Hiramine, On planar functions, J. Algebra 133 (1990) 103–110.
[15] W.M. Kantor, Commutative semifields and symplectic spreads, J. Algebra 270 (2003) 96–114.
[16] D.E. Knuth, Finite semifields and projective planes, J. Algebra 2 (1965) 182–217.
[17] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monogr. Surv. Pure Appl. Math., vol. 65, Longman Scientific and Technical, Essex, England, 1993.
[18] G. Menichetti, On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field, J. Algebra 47 (1977) 400–410.
[19] E.H. Moore, A doubly-infinite system of simple groups, Bull. New York Math. Soc. 3 (1893) 69–82.
[20] E.H. Moore, A doubly-infinite system of simple groups, in: Math. Papers read at the Congress of Mathematics, Chicago, 1893, 1896, pp. 208–242.
[21] T. Penttila, B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (2000) 1–19.
[22] L. Rónyai, T. Szőnyi, Planar functions over finite fields, Combinatorica 9 (1989) 315–320.
[23] J.H.M. Wedderburn, A theorem on finite algebras, Trans. Amer. Math. Soc. 6 (1905) 349–352.